UNIVERSIDAD DEL BIO-BIO
FACULTAD DE CIENCIAS EMPRESARIALES
ESCUELA DE INGENIERÍA CIVIL INFORMÁTICA

CERTAMEN 2 - PAUTA
Seguridad Informática

Prof. María Antonieta Soto Ch., 10/12/2018

Nombre: _____ Pje./Nota: _____

PARTE I. preguntas y Respuestas
Indicaciones generales: SEA PRECISO Y CONCISO EN SUS RESPUESTAS

1. Defina los siguientes términos: (28 pts., 4 pts. c/u)
   a) Vulnerabilidad de cero días.
   b) Ransomware.
   c) DDoS.
   d) Ataque de Saturación de Búfer.
   e) Inyección SQL.
   f) Honeypot.
   g) Ventajas y desventajas del uso de sellos de tiempo en protocolos de autenticación.

   R:
   a) Vulnerabilidad de cero días es una vulnerabilidad presente en un software que los proveedores o creadores y los usuarios del mismo desconocen y para el cual no existe solución. Se da usualmente al liberar un nuevo producto una nueva versión de un software.
   b) Ransomware es un ataque en el que los datos de una persona o empresa se secuestran (cifran) y se devuelven (dan clave de descifrado) al pagar (transferir) una suma de dinero.
   c) Ataque de denegación de servicio distribuido (DDoS) consiste en utilizar grupos de equipos, llamados zombies, los cuales dejan a un servidor inhabilitado (usualmente) para atender a sus usuarios o clientes autorizados, al mantenerlo excesivamente ocupado o provocar que cese sus servicios del todo.
   d) Ataque de saturación de búfer consiste en acceder a espacios de memoria no permitidos borrando o modificando su contenido. P.e., acceder a la pila de llamadas/retornos del S.O, borrando la dirección de retorno requerida o modificando dicha dirección para lograr que el host ejecute un código malicioso.
   e) Inyección SQL. Ataque en el que se ingresa, como dato, una sentencia SQL que permita leer o modificar (incluso borrar) la BD de un servidor.
   f) Honeypot es una trampa, un host señuelo para que sea atacado y, de este modo, detectar información del ataque y del atacante.
   g) Ventajas del uso de sellos de tiempo en protocolos de autenticación: permite establecer frescura de un mensaje y detectar su reutilización.
      Desventaja: Los relojes de los hosts nunca están sincronizados, se debe permitir un margen, lo que es una oportunidad de reuso de mensajes.

2. Respecto de IPTABLES y SNORT: (14 pts.)
   a) Dé un ejemplo para IPTABLEs y otro para SNORT de una posible regla para evitar/alertar de tráfico enviado desde un sitio remoto identificado por la dirección IP w.x.y.z (6)
      R:
      iptables –A INPUT –s w.x.y.z –j DROP
      Snort –-> alert ip w.x.y.z any -> any any (msg: “Paquete IP detectado”;)

   b) Especifique una regla de IPTABLEs para aceptar HTTP enviado a un servidor con dirección IP a.b.c.d desde cualquier sitio remoto (5)
      R:
      iptables –A INPUT –d a.b.c.d –p tcp -dport 80 –j ACCEPT

   c) Especifique una regla de IPTABLEs que establezca que, por defecto, todos los paquetes son descartados (drop). (3)
      R:
      iptables -P INPUT DROP
      iptables -P FORWARD DROP
      iptables -P OUTPUT DROP

3. Explique si es posible con NMAP conocer los hosts que componen una red objetivo y también averiguar los servicios que corren estos mismos hosts. Si su respuesta es afirmativa, describa cómo NMAP puede hacerlo; en caso contrario, explique en qué aspectos la herramienta falla o es incompleta. (10 pts.)

   R: nmap cuenta con opciones que le permiten descubrir hosts activos, en particular el siguiente comando:

   Nmap –sP a.b.c.d/cdir

   Retorna los hosts activos de la red indicada.

   Luego, se puede realizar escaneo para que retorne los puertos activos y los servicios que corren en ellos. Uno de esos comandos es: nmap host1, host2,… que permite escanear varios hosts de interés.

4. Considere la pila de protocolos TCP/IP (incluya capa de enlace). Describa, al menos**, un potencial ataque** a **cada una de las capas** de la pila. Sugiera **alguna** solución para mitigar tal ataque (12 pts.)

   R:

   Capa de enlace -> Fraude o envenenamiento ARP. / **Sol**.: Tabla ARP estática, certificación DHCP, detección con Arpwatch

   Capa de red -> Sniffing de paquetes IP (tarjetas de red promiscuas). / **Sol**: prevención mediante cifrado (IPSec y TLS)

   Capa de transporte -> Secuestro ciego de sesión TCP. /**Sol**.: Uso de firewall para proteger servidor y cliente, SSL y SSH.

   Nota: Ataques a partir del secuestro de sesión: Inyección de datos servidor-servidor, inyección de datos en tráfico cliente a servidor, falsificación de IPs, ataques MiTM, denegación de servicio)

   Capa de aplicación ->

   - Ataques a DNS; Pharming (lado cliente) / **Sol**.: Id de transacción DNS aleatorio.
   - Envenenamiento de caché de DNS / **Sol**.: Uso de reglas de Bailiwicks.
   - Envenenamiento de caché de DNS (ataque de cumpleaños, Kaminsky) / **Sol**.: Cambiar servidor recursivo (local), aleatorización de puerto de origen, DNSSec, DNSCurve.

5. Considere la red de la Figura 1. Se desea que usuarios corporativos puedan acceder desde sus casas a la red corporativa de la empresa ACME. (10 pts.)

   ¿En qué lugares instalaría cortafuegos? Utilice, si desea, la misma figura para graficar donde instalaría estos recursos. Justifique su respuesta indicando a qué tipo de adversarios pretende detectar y/o controlar.

   R:

   Justificación: Se ubican los cortafuegos en las líneas provenientes de Internet, incluyendo la que implementa VPN (pues esta tecnología permite autenticación, pero no impide intrusiones). El propósito es proteger a la empresa de adversarios externos, así como de la fuga de información desde el interior de la empresa.

   Observación: La línea que va a la casa del empleado que trabaja a distancia no es responsabilidad de la empresa, sino del ISP que contrata el empleado.

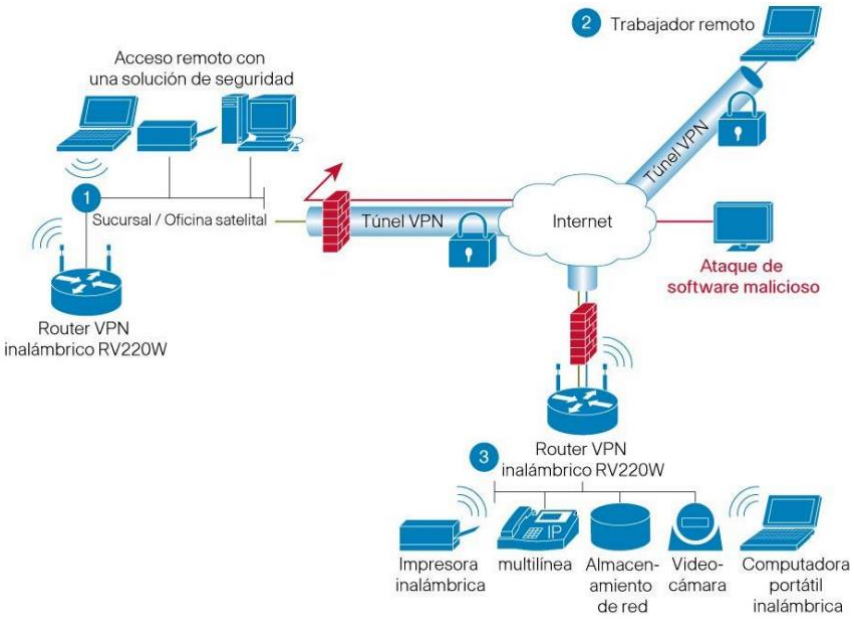


Figura 1: Red de la Empresa ACME

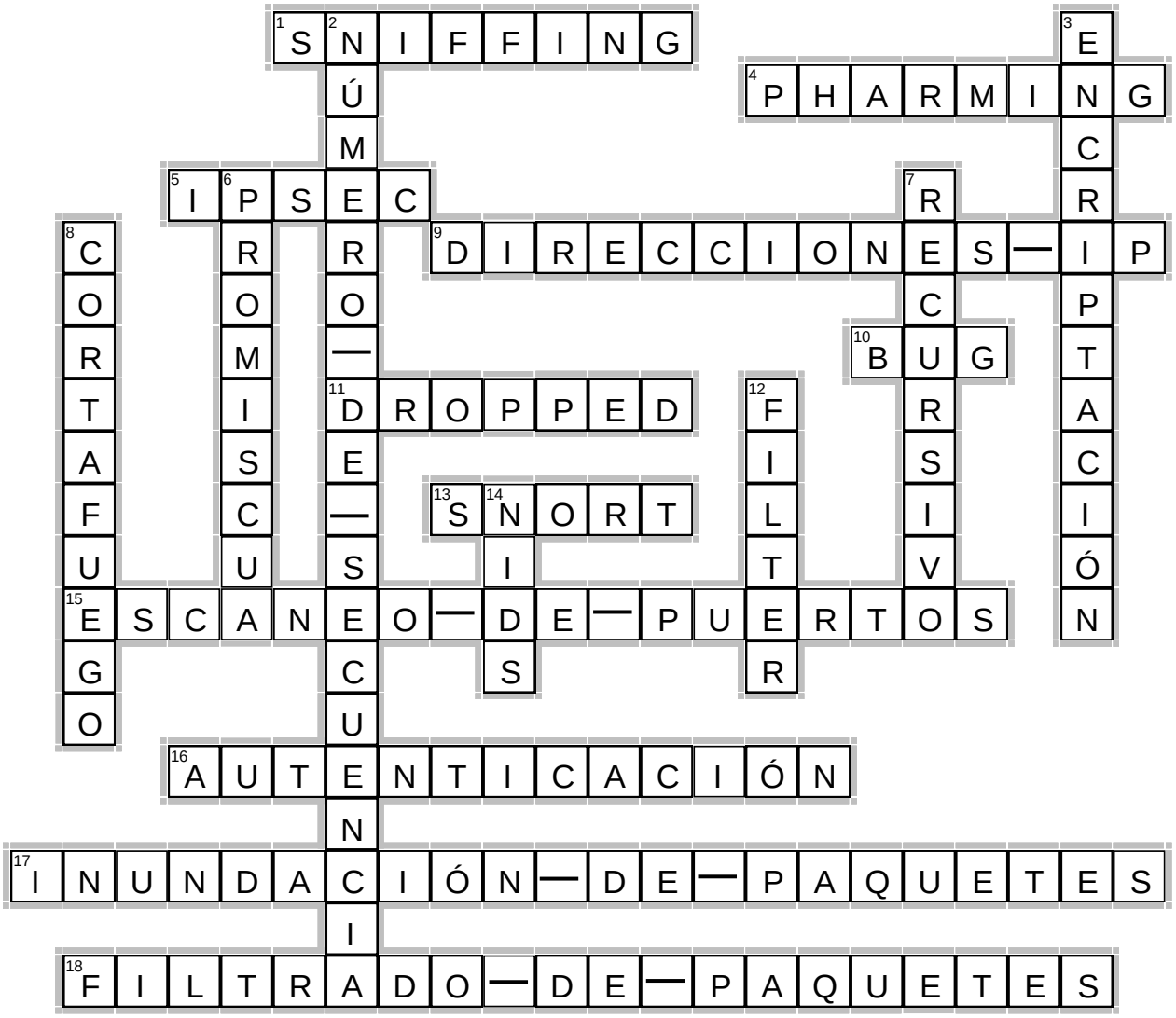
PARTE II. Palabras cruzadas

Horizontal

1. Ataque que sufren los datagramas IP al avanzar por los saltos de una red.
4. Nombre dado a un tipo de ataque DNS del lado del cliente.
5. Conjunto de protocolos que permiten asegurar los datagramas IP.
9. Aquello asociado a la MAC del atacante en el envenenamiento de ARP.
10. Nombre dado, en inglés, a una equivocación al programar.
11. Una de las salidas que pueden tener lo paquetes que fluyen por un cortafuegos (en inglés).
13. Es un sistema de prevención y detección de intrusiones de red de código abierto. Utiliza un lenguaje basado en reglas que combina métodos de inspección de firmas, protocolos y anomalías.
15. Es el análisis, por medio de una aplicación, del estado de los puertos de una máquina conectada a una red.
16. Proceso o procedimiento no implementado en ARP que permite su envenenamiento.
17. Ataque de denegación de servicio remoto consistente en agotar recursos.
18. Un tipo o modalidad en la que se puede definir o implementar un cortafuego.

Vertical

2. Campo de las unidades datos TCP que, dada su posible predicción, permite la inyección de datos falsos en la red.
3. Medida que permite prevenir el ataque a protocolos IP.
6. Nombre dado a la característica de una tarjeta de interfaz de red cuando lee todas las tramas y no solo los destinados a ella.
7. Uno de los dos esquemas de resolución de nombre de dominio usado por DNS
8. Colección integrada de medidas de seguridad diseñadas para evitar el acceso electrónico no autorizado a un sistema informático en red.
12. Una de las tres tablas construidas por defecto para el procesamiento de paquetes en iptables (en inglés).
14. Sigla para Sistema de detección de intrusiones de red (en inglés).


1 SNIFFING
2 NÚMERO—DE—SECUENCIA
3 E
4 PHARMING
5 IP
6 SPOOFING
7 R
8 CORTAFUEGOS
9 DIRECCIONES—IP
10 BUG
11 DROPPED
12 FILTRADO
13 SNORT
14 NIDS
15 ESCANEO—DE—PUERTOS
16 AUTENTICACIÓN
17 INUNDACIÓN—DE—PAQUETES
18 FILTRADO—DE—PAQUETES
EclipseCrossword.com

ANEXO

NMAP CHEAT SHEET

Tips for conducting a Nmap scan.

Basic Scanning Techniques	
Scan a single target	nmap [target]
Scan multiple targets	nmap [target1,target2,etc]
Scan a list of targets	nmap -iL [list.txt]
Scan a range of hosts	nmap [range of IP addresses]
Scan an entire subnet	nmap [IP address/cdir]
Scan random hosts	nmap -iR [number]
Excluding targets from a scan	nmap [targets] –exclude [targets]
Excluding targets using a list	nmap [targets] –excludefile [list.txt]
Perform an aggressive scan	nmap -A [target]
Scan an IPv6 target	nmap -6 [target]

Discovery Options	
Perform a ping scan only	nmap -sP [target]
Don't ping	nmap -PN [target]
TCP SYN Ping	nmap -PS [target]
TCP ACK ping	nmap -PA [target]
UDP ping	nmap -PU [target]
SCTP Init Ping	nmap -PY [target]
ICMP echo ping	nmap -PE [target]
ICMP Timestamp ping	nmap -PP [target]
ICMP address mask ping	nmap -PM [target]
IP protocol ping	nmap -PO [target]
ARP ping	nmap -PR [target]
Traceroute	nmap –traceroute [target]
Force reverse DNS resolution	nmap -R [target]
Disable reverse DNS resolution	nmap -n [target]

Advanced Scanning Options	
TCP SYN Scan	nmap -sS [target]
TCP connect scan	nmap -sT [target]
UDP scan	nmap -sU [target]
TCP Null scan	nmap -sN [target]
TCP Fin scan	nmap -sF [target]
Xmas scan	nmap -sX [target]
TCP ACK scan	nmap -sA [target]
Custom TCP scan	nmap –scanflags [flags] [target]
IP protocol scan	nmap -sO [target]
Send Raw Ethernet packets	nmap –send-eth [target]
Send IP packets	nmap –send-ip [target]

Port Scanning Options	
Perform a fast scan	nmap -F [target]
Scan specific ports	nmap -p [ports] [target]
Scan ports by name	nmap -p [port name] [target]
Scan ports by protocol	nmap -sU -sT -p U:[ports],T:[ports] [target]
Scan all ports	nmap -p "*" [target]
Scan top ports	nmap –top-ports [number] [target]
Perform a sequential port scan	nmap -r [target]

Version Detection	
Operating system detection	nmap -O [target]
Attempt to guess an unknown	nmap -O –osscan-guess [target]
Service version detection	nmap -sV [target]
Troubleshooting version scans	nmap -sV –version-trace [target]
Perform a RPC scan	nmap -sR [target]

Timing Options	
Timing Templates	nmap -T [0-5] [target]
Set the packet TTL	nmap –ttl [time] [target]
Minimum of parallel connections	nmap –min-parallelism [number] [target]
Maximum of parallel connection	nmap –max-parallelism [number] [target]
Minimum host group size	nmap –min-hostgroup [number] [targets]
Maximum host group size	nmap –max-hostgroup [number] [targets]
Maximum RTT timeout	nmap –initial-rtt-timeout [time] [target]
Initial RTT timeout	nmap –max-rtt-timeout [TTL] [target]
Maximum retries	nmap –max-retries [number] [target]
Host timeout	nmap –host-timeout [time] [target]
Minimum Scan delay	nmap –scan-delay [time] [target]
Maximum scan delay	nmap –max-scan-delay [time] [target]
Minimum packet rate	nmap –min-rate [number] [target]
Maximum packet rate	nmap –max-rate [number] [target]
Defeat reset rate limits	nmap –defeat-rst-ratelimit [target]